How to support both legacy and mobile SSL clients by using ECDSA and RSA certificates together on NetScaler ADC?

Use Case

Support legacy and mobile clients on SSL virtual servers on NetScaler by using ECDSA and RSA certificates together.

Introduction

RSA certificates have been popular for decades now. While traditional clients are able to perform well with RSA certificates, devices like smartphones and other handheld devices are slow in processing RSA certificates due to the limited CPU processing and battery power. The problem increases due to the need to use larger RSA key size (>2048-bit) to make the connection secure.

The problem is solved with Elliptic Curve Cryptography (ECC) certificates which are small in size and provides same level of security as RSA certificates. Elliptic Curve Digital Signature Algorithm (ECDSA) is an asymmetric algorithm using ECC and is used for certificate signing purpose. ECDSA signed certificates are small in size (256-bits or 384-bits) and suitable for mobile devices.

Today, most of the servers will have both legacy as well as modern clients connecting. It therefore becomes important for servers to support both RSA and ECDSA signed certificates on servers. NetScaler supports coexistence of an RSA and an ECDSA certificate on a SSL type virtual servers of type load balancing, content witching and Gateway. Based on the client information received in Client Hello (supported ciphers and signature extensions), NetScaler virtual server will intelligently select one of the two certificates and send the appropriate one to the clients.

Configuration Steps in NetScaler ADC

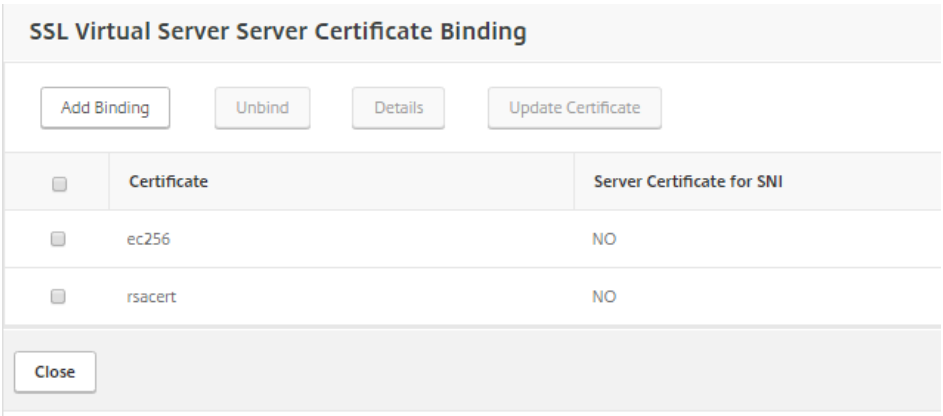
Step 1: Install server certificates

Both RSA and ECDSA certificates shall be installed as server certificates on the NetScaler appliance. See how to install a certificate on NetScaler here - How do I upload different types of certificates on NetScaler.

Step 2: Bind certificates to SSL virtual server

Bind both RSA and ECDSA server certificates to the SSL type virtual server. Know how to bind a certificate to a virtual server here - How do I bind an SSL certificate to a vServer on NetScaler.

Once the two server certificates are bound, the bindings screen should look like this –



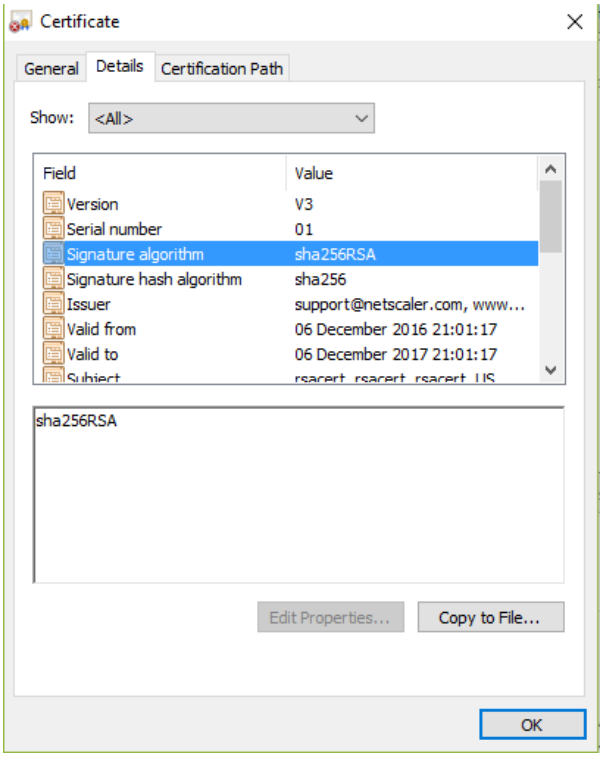
Validation

Validate if the server is sending the appropriate server certificate to the client by looking for SSL connection information on client.

Scenario 1:

Legacy client which supports RSA certificates only connects to the SSL virtual server on NetScaler.

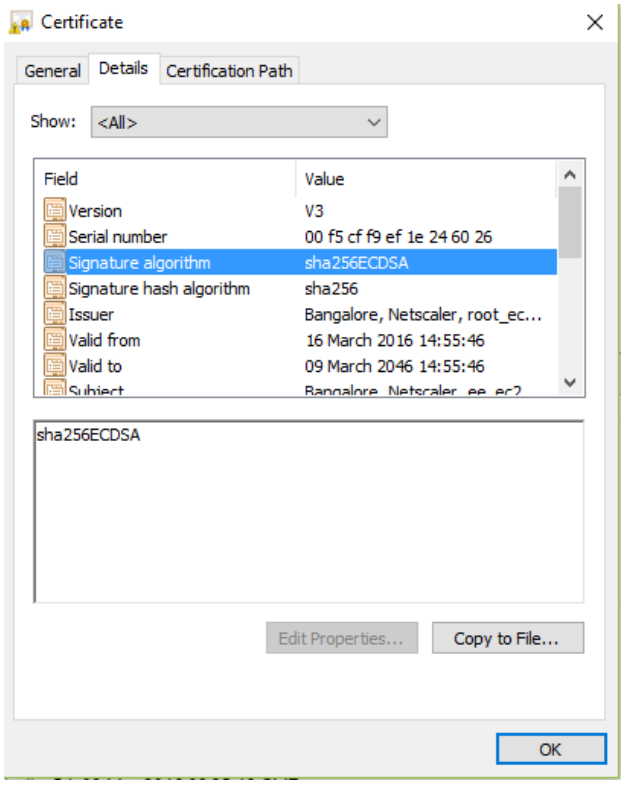
As seen in the screenshots below, RSA server certificate is sent by the virtual server to this client and following which the SSL handshake completes.



Scenario 2:

Modern client which supports ECDSA certificates connects to the SSL virtual server on NetScaler.

As seen in the screenshot below, ECDSA server certificate is sent by the virtual server to the client.



Also, in the connection details on the client side, key exchange algorithm is seen as ECDHE-ECDSA.